중복된 JSON 이벤트.

적용 가능성

Splunk Enterprise

조사

btool 명령을 실행하고 KV _MODE 및 AUTO_KV_JSON 특성을 검색할 때는 json 및 true로 각각 설정됩니다.

```
splunk btool props list --debug <my_sourcetype_name>
/opt/splunk/etc/system/default/props.conf                    ADD_EXTRA_TIME_FIELDS = True
/opt/splunk/etc/system/default/props.conf                    ANNOTATE_PUNCT = True
/opt/splunk/etc/system/default/props.conf                    AUTO_KV_JSON = True  <======
/opt/splunk/etc/system/default/props.conf                    BREAK_ONLY_BEFORE =
/opt/splunk/etc/system/default/props.conf                    BREAK_ONLY_BEFORE_DATE = Tru
/opt/splunk/etc/system/default/props.conf                    CHARSET = UTF-8
/opt/splunk/etc/apps/search/local/props.conf                 DATETIME_CONFIG =
/opt/splunk/etc/apps/search/local/props.conf                 INDEXED_EXTRACTIONS = json
```

해결

문서에 따르면:

"참고: INDEXED_*EXTRACTIONS=JSON*을 설정하는 경우 동일한 소스 유형에 대해 KV_*MODE = json*을 설정하지 않았는지 확인하십시오. 그러면 인덱스 시간과 검색 시간에 JSON 필드가 두 번 추출됩니다."

따라서 문제를 중지하려면 특성 중 하나를 비활성화해야 합니다.

AUTO_KV_JSON(검색 시간 필드 추출)
INDEXED_EXTRACTION(인덱스 시간 추출)

관련 링크

Splunk Answers

내 json 필드가 두 번 추출된 이유는 무엇입니까?
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Splunk 설명서

구조화된 데이터의 Props.conf 속성
https://docs.splunk.com/Documentation/Splunk/8.0.0/Data/Extractfieldsfromfileswithstructureddata#Props.
default.meta.conf

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Defaultmetaconf#default.meta.conf.spec
props.conf.spec https://docs.splunk.com/Documentation/Splunk/8.0.0/Admin/Propsconf

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.